UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/700,656	02/14/2001	Harald Vater	JEK/VATER	7577

7590 02/22/2005

Bacon & Thomas
Fourth Floor
625 Slaters Lane
Alexandria, VA 22314-1176

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 02/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/700,656	VATER ET AL.	
	Examiner	Art Unit	
	Zachary A Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 September 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. An amendment was received on 23 September 2004. Claims 1-41 have been amended. New claims 42 and 43 have been added. No claims have been canceled. Claims 1-43 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments with respect to the rejections of claims 1-4, 13-25, and 34-41 under 35 U.S.C. 102(e) as being anticipated by Candelore et al, US Patent 6061449, and 1, 5-12, 21, 22, and 26-33 under 35 U.S.C. 102(e) as being anticipated by Johnston, US Patent 6373946, have been considered but are moot in view of the new ground(s) of rejection.

3. The Examiner thanks Applicant for the further clarification of the terms "falsification" and "compensation". Although it is clear that compensation does not directly correspond to decryption, the Examiner submits that Applicant's definition of falsification does indeed fall under the scope of encryption. Indeed, one of the simplest forms of encryption is simply to bitwise XOR a random key with the plaintext (in this case, the secret key) in order to form a ciphertext. For example, see Schneier, *Applied Cryptography,* pages 16-17. Nevertheless, the rejections of claims 5, 6, 26, and 27 are withdrawn, as noted above.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-4, 13-25, and 34-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore et al, US Patent 6061449, in view of Dunlavy, US Patent 5297201.

In reference to Claim 1, Candelore discloses a data carrier with a semiconductor chip having a memory storing an operating program composed of commands, in which the data carrier performs security-related operations such that the data being processed cannot be determined from detected signals produced by the chip (column 17, lines 59-67). However, Candelore does not explicitly disclose that the detected signals are detected from radiation outside the semiconductor chip.

Dunlavy discloses a system for preventing remote detection of data from radiated signals (column 2, lines 25-31; note also column 8, lines 11-27). Specifically, Dunlavy discloses making it difficult to distinguish executed commands from the emissions radiated by the chip when executing (column 6, lines 42-47). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the data carrier of Candelore to include Dunlavy's method of making emissions

of commands indistinguishable, in order to prevent decoding of the emissions to obtain sensitive data (see Dunlavy, column 3, lines 32-37).

In reference to Claim 2, Candelore further discloses that commands perform byte-by-byte processing (column 17, lines 59-67).

In reference to Claims 3 and 4, Dunlavy further discloses that commands are indistinguishable with respect to the signal patterns caused by the commands, and lead to a signal pattern that is substantially independent of the data processed (column 5, lines 33-45; column 5, line 62-column 6, line 7; column 6, lines 40-53).

In reference to Claim 13, Candelore further discloses that the order of execution of operations can be varied (column 22, lines 3-14).

In reference to Claim 14, Candelore further discloses that the order of execution is varied at each run (column 23, lines 19-22).

In reference to Claims 15 and 16, Candelore further discloses that the order of execution can be varied according to a fixed principle or randomly (column 23, lines 3-6, where the numbers can be either random or pseudo-random).

In reference to Claim 17, Candelore further discloses that the order of execution can be varied based on the data to be processed (column 14, lines 59-63; column 15, lines 23-25).

In reference to Claims 18 and 19, Candelore further discloses that the order of execution can be fixed before execution of a first operation (column 15, lines 19-21) or before execution of a next operation (column 23, lines 30-34).

In reference to Claim 20, Candelore further discloses that the security-related operations are permutations of data (column 17, lines 61-64).

In reference to Claim 21, Candelore further discloses a smart card (column 18, lines 17-22).

Claims 22-25 and 34-41 are method claims that correspond substantially to Claims 1-4 and 13-20, and are rejected by a similar rationale. Claims 42 and 43 recite the same limitation as Claims 20 and 41 and are also rejected by a similar rationale.

6. Claims 5-12 and 26-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore in view of Dunlavy as applied to Claims 1 and 22 above, and further in view of Johnston, US Patent 6373946.

In reference to Claim 5, Candelore as modified by Dunlavy discloses everything as applied to Claim 1 above. However, neither Candelore nor Dunlavy explicitly discloses combining input or output data with auxiliary data values. Johnston discloses a data carrier with a semiconductor chip and a memory that is designed to perform security-related operations (column 6, lines 20-23). Johnston further discloses that the operating program includes combining input data with auxiliary data (column 9, line 66-column 10, line 8) and combining output data with an auxiliary function value (column 10, lines 38-42). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify further the data carrier of Candelore as modified by Dunlavy by including the combination of input data with auxiliary data and

output data with an auxiliary function value, in order to decrease the risk of data being obtained by eavesdropping (see Johnston, column 2, lines 53-67).

In reference to Claim 6, Johnston further discloses that the combination with the auxiliary function value is done before performing a non-linear operation (column 10, lines 51-53).

In reference to Claim 7, Johnston further discloses that the auxiliary data are varied (column 11, lines 20-23).

In reference to Claims 8-11, Johnston further discloses that new auxiliary values can be generated by combining existing values, that auxiliary data are selected randomly, pairs of auxiliary data and auxiliary function values are generated, and the auxiliary data are random numbers (column 9, lines 61-65, where the numbers are pseudo random).

In reference to Claim 12, Johnston further discloses that the combination is an exclusive OR operation (column 9, line 66-column 10, line 12).

Claims 26-33 are method claims that correspond substantially to Claims 5-12, and are rejected by a similar rationale.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Matsumura et al, US Patent 4908038, discloses an integrated circuit card that defends against cryptanalytic timing attacks.

b. Fruhauf et al, US Patent 4932053, discloses a circuit to protect chip cards from cryptanalytic attacks depending on analysis of current consumption in the device.

c. Shamir, US Patent 5991415, discloses an apparatus for protecting encryption devices, such as smart cards, from cryptanalytic timing and fault attacks.

d. Jakobsson, US Patent 6049613, discloses a method and apparatus for protecting data values that includes blinding data before performing cryptographic operations on the data.

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER